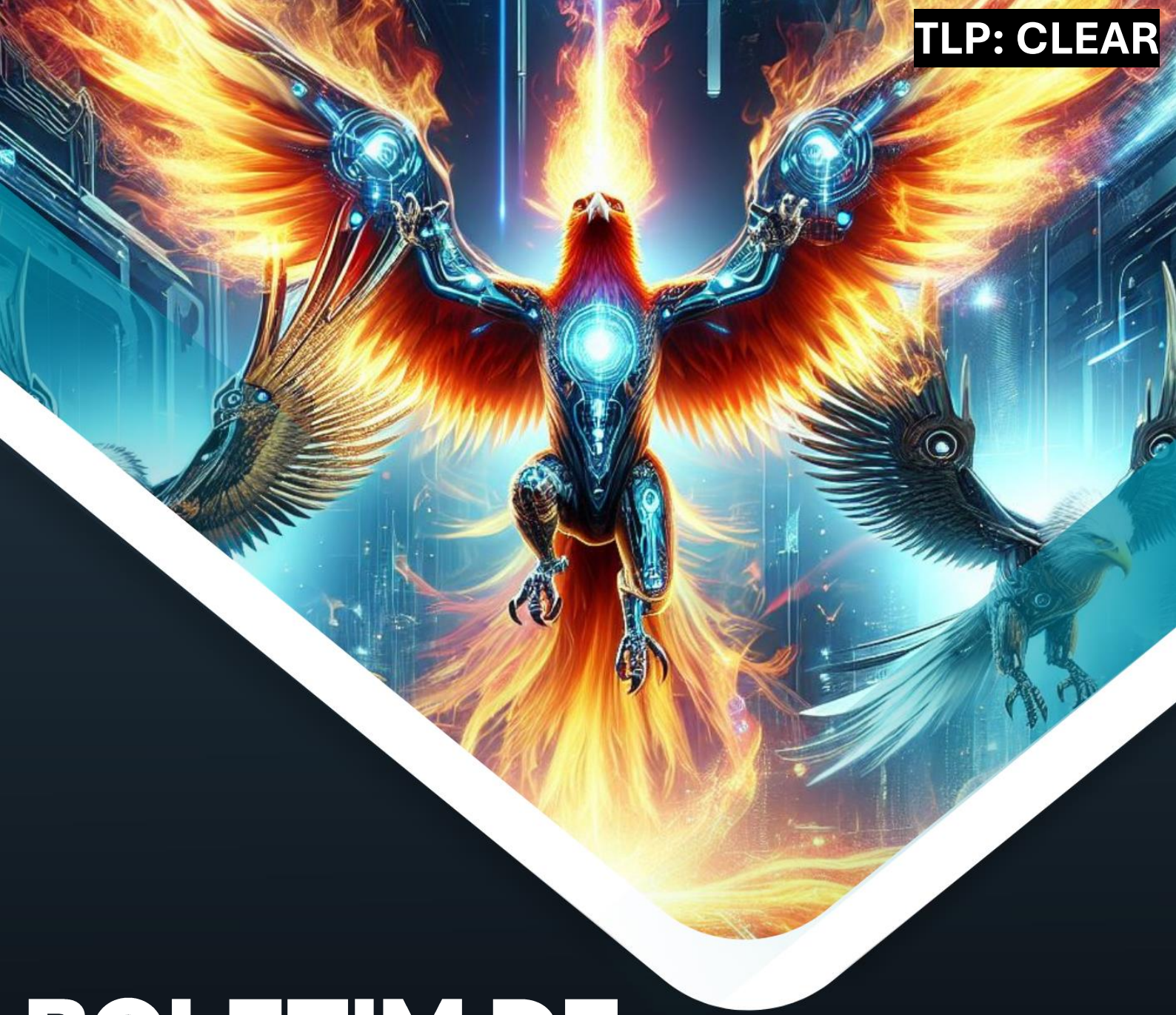
TLP: CLEAR



BOLETIM DE SEGURANÇA

Spyware Chinês EagleMsgSpy explorando dispositivos móveis desde 2017

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

heimdall
security research
A DIVISION OF ISH

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INFORMAÇÕES SOBRE A AMEAÇA

Pesquisadores identificaram uma nova família de *spyware* denominada **EagleMsgSpy**, que se trata de um software de vigilância desenvolvido por uma empresa chinesa de software, utilizado por agências de segurança pública na China continental. Este software coleta uma vasta gama de dados do usuário, incluindo mensagens de aplicativos de terceiros, gravações e capturas de tela, gravações de áudio, registros de chamadas, contatos, mensagens SMS, dados de localização e atividade de rede. Conforme relatado, evidências iniciais mostram que essa ferramenta está em operação desde pelo menos 2017, com desenvolvimento contínuo até o final de 2024. O software é composto por duas partes: um instalador APK e um cliente de vigilância que opera sem interface gráfica no dispositivo.

Figura 1 – Instalador apresentando ao usuário diversas opções para instalar.

A carga de vigilância reúne uma vasta quantidade de informações sobre o dispositivo da vítima:

- *O Notification Listener e os Serviços de Acessibilidade monitoram o uso do dispositivo e interceptam mensagens recebidas*.
- *Coleta todas as mensagens de aplicativos como QQ, Telegram, Viber, WhatsApp e WeChat*.
- *Inicia a gravação da tela do dispositivo através do serviço de projeção de mídia*.
- *Realiza capturas de tela*.
- *Grava áudios do dispositivo durante o uso*.
- *Coleta registros de chamadas*.
- *Reúne contatos do dispositivo*.
- *Coleta mensagens SMS*.
- *Compila uma lista dos aplicativos instalados no dispositivo*.
- *Recupera coordenadas GPS*.
- *Detalha conexões de rede e Wi-Fi*.
- *Compila uma lista de arquivos armazenados externamente*.
- *Coleta os favoritos do navegador do dispositivo*.

Dessa forma, o aplicativo consegue monitorar e registrar uma ampla gama de atividades e informações do dispositivo. Após a coleta dos dados, eles são armazenados em uma área de preparação dentro de um diretório oculto no sistema de arquivos do dispositivo, aguardando possível exfiltração. Esses arquivos são então compactados e protegidos por senha antes de serem enviados ao servidor de comando e controle (C2). Os servidores C2 do EagleMsgSpy possuem um painel administrativo que exige autenticação do usuário.

```
function getListIOS() {
    var _param = {
        collect_target_id: _collect_target_id,
        type: routeType
    };
    vm.isLoading = true;
    IM.getAccountInfo(_param).then(
        function (result) {
            vm.isLoading = false;
            if (result.data.retcode === 1) {
                if (result.data.data.last_sync_time) vm.lastSyncTime = result.data.data.
                last_sync_time;
                $rootScope.$broadcast('setLastSyncTime', vm.lastSyncTime);
                if (result.data.data.account.length > 0) {
                    vm.list = result.data.data.account;  // 得到登录的3个QQ账号
                    if (vm.list.length > 0) {
                        handelList();
                        // vm.currentAccount.nickname = vm.list[0].nickname;
                        // vm.currentAccount.accountId = vm.list[0].account;

                        // $state.go('home.device.im.' + vm.routeType + '.account', {
                        //     id: vm.navId,
                        //     accountId: vm.currentAccount.accountId
                        // });
                    }
                }
            }
        },
        function () {
            vm.isLoading = false;
        }
    )
}
```

Figura 2 – Função, getListIOS(), de /assets/js/controller/device/im.js.

Um dos servidores C2 identificados tinha um endereço IP que já havia sido vinculado a diversos subdomínios pertencentes a uma empresa privada de tecnologia da China, a Wuhan Chinasoft Token Information Technology Co., Ltd.

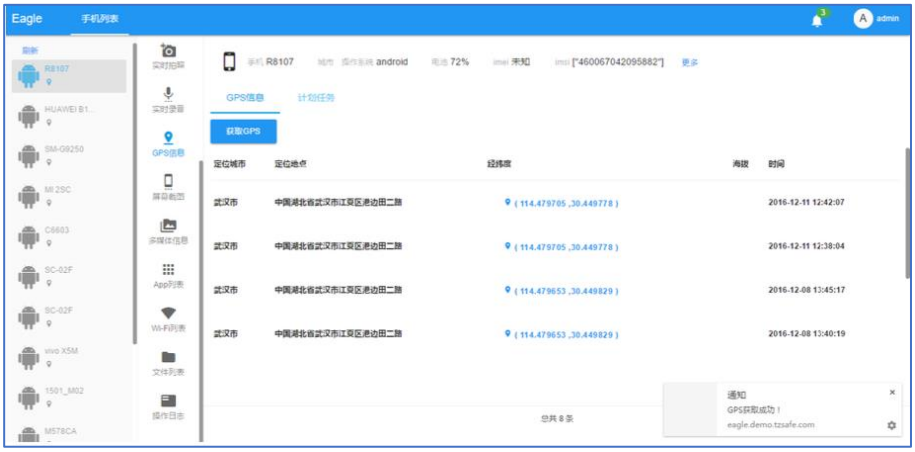


Figura 3 – Captura de tela do painel de análise GPS.

Ferramentas de vigilância chinesas conhecidas reutilizaram a infraestrutura de certificados SSL dos servidores EagleMsgSpy C2 em campanhas anteriores. O endereço IP 202.107.80[.]34 foi associado a 15 amostras do PluginPhantom, utilizadas de 2017 a 2020 por APTs chineses. Uma amostra do CarbonSteal, uma ferramenta de vigilância identificada pela Lookout e atribuída a APTs chineses, foi vista comunicando-se com outro IP relacionado ao certificado SSL EagleMsgSpy.

2 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Mantenha seu software atualizado

- Certifique-se de que todos os seus dispositivos e aplicativos estejam sempre com as últimas atualizações de segurança instaladas.

Use autenticação de dois fatores (2FA)

- Adicione uma camada extra de segurança às suas contas online, exigindo um segundo fator de autenticação além da senha.

Evite clicar em links desconhecidos

- Não clique em links ou abra anexos de e-mails ou mensagens de remetentes desconhecidos, pois eles podem conter malware.

Utilize uma VPN

- Uma rede privada virtual (VPN) pode ajudar a proteger sua conexão à internet, tornando mais difícil para espiões interceptarem seus dados.

Instale software antivírus e antimalware

- Use programas confiáveis para detectar e remover ameaças de spyware e outros tipos de malware.

Desative a execução automática de mídias

- Configure seus dispositivos para não executarem automaticamente mídias removíveis, como pendrives, que podem estar infectadas.

Monitore suas contas e dispositivos

- Fique atento a atividades suspeitas em suas contas e dispositivos, como logins não reconhecidos ou comportamento estranho do sistema.

3 INDICADORES DE COMPROMETIMENTO (IOC)

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores do artefato	
md5:	5792a8771239028bee7037175d914ae2
sha1:	5d935d5ab7b7c6b301a4c79807c33e0bee23e3ff
sha256:	5498ba054cc81d9f5231a05f368330477655baefc3197aceae854a5f7befc43e
File name:	detect.apk

Indicadores do artefato	
md5:	fdd15a9bdf23eef8ca90e19256737df4
sha1:	dab40467824ff3960476d924ada91997ddfce0b0
sha256:	3208faa2e71709b367e59ef7879aee5a503e1cbafbd82458d316097ed16276b6
File name:	=?UTF-8?B?57O757uf5pyN5YqhLmFwaw==?=

Indicadores do artefato	
md5:	7221d298941f73df978c04cab02e4eac
sha1:	5208039ef9efb317cc2ed7085ca98386ec31b0b4
sha256:	b33bdb6cc8f48c92b10c22b6e98ac64ef8bf52375ff05eeeabe3fc5a4140404d
File name:	7221d298941f73df978c04cab02e4eac.vírus

Indicadores do artefato	
md5:	6fe4bbac94761250127ef17cb600fa53
sha1:	9557eebe4ee2dc602750365e722002d9f686b7fb
sha256:	bbfe8346fb42baff29b6bf4cc3c1d545a2719d11850582b8474094f9ef940377
File name:	6FE4BBAC94761250127EF17CB600FA53.apk

Tabela 1 – Indicadores de Comprometimento

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Lookout**
- **Thehackernews**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH